[0023] Presently, and generally speaking, there is a number of challenges aiming the present invention to overcome the mostly common and some particular drawbacks from these two approaches.

[0024] A first drawback to deal with is that a single operator's user typically has a large number of identities at both network operator and service providers, and in most of the cases a user has an identity per each subscribed service. In this respect, temporary and permanent user's identities in each service namespace have to be unique in order to let each service have a key to create accounts. Moreover, two different users cannot have the same identity, either temporary or permanent, for the same or different services in order to let the operator connect the identity to the actual user it belongs to. Furthermore, identities for a same user must be different in order to prevent external service providers to create some kind of user profile by linking data from different services. Thus, there is a huge number of user's identities and identifiers to be stored in a user directory accessible to the network operator acting as Identity Provider. As the number of subscribers grow and the use of services increases, the huge number of user's identities and identifiers to be stored in a user directory becomes a problem for the operators in this sort of scenarios.

[0025] A second drawback is that, currently, some knowledge about the actual end-user's identity in the real world can be extracted from the user's identity in the telecommunication world. For example, the International Publication WO 03/050743 shows how an alias is generated in an entity of the Identity Provider, from a user identity and a service identifier, and submitted to a Content Provider where the user identity is extracted. In this respect, both temporary and permanent users' identities have to be opaque for the services. This feature is usually due to regulatory and privacy constraints. Thereby, the handling of user's identities by the operators requires a large number of indices, what introduces big performance penalties and is also a problem addressed by the present invention. Even if a unique alias is used between the Identity Provider (IDP) and the Service Provider (SP), as the alias is the sole identity referring to an end-user in all communications between two actors such as service providers and identity providers, the alias can be considered a primary key for searching in their respective databases for said user's profile. For example, the publication US 2003/0093681 shows how an authorization token is generated, also from a user identity and a service identifier, and said token further compared with a token stored in a directory system, the authorization token being used as the search key in said directory. Administration and storage of aliases or pseudonyms in databases at each actor, especially at the identity provider, which in particular might be an operator, would be difficult once the number of aliases per user increases above a certain threshold value. This fact also has a negative impact on the performance of database operations, especially search or lookup operations.

[0026] On the other hand, another challenge of the invention is the protection of users from malicious Service Providers that create services delivering contents to the users without having been requested. As these services are usually premium ones, this misbehaviour let those Service Providers get revenues for non-requested contents. As a consequence, further challenges turn up over the ones mentioned above in respect of handling the user's identity management and services without a user account.

[0027] A first additional challenge is that a service should not be able to "guess" valid temporal identities in order to prevent malicious services from delivering contents, which had not been requested, by using a "guessed" temporal identity. Another additional challenge is that a temporary identity must have a limited lifetime in order to prevent malicious services from delivering contents that had not been requested by using an old temporary identity. A further additional challenge is the provision of a simpler method to verify whether a temporary identity is still valid. Moreover, these challenges must be accomplished in a manner that the impacts on the operator's database systems are minimised.

CLAIMS

1. An Identity Generator device (6) arranged for generating a user's service indicator (USI) for a user to access a number of services offered by a service provider (1; 2; 3) through a network operator where user data (4) for the user are accessible in a user directory system (4), this user's service indicator being usable between the service provider (SP-1; SP-2; SP-N) domain and the network operator (IDP) domain to unambiguously identify the user at each respective domain, the Identity Generator device comprising:

   – means for obtaining a master user's identifier (UID) usable to identify the user at the operator's network;

   – means for obtaining a service identifier (SID), indicative of services to be accessed at the service provider; and

   – means (F) for constructing a user's service indicator (USI) that includes the master user's identifier (UID) and the service identifier (SID);

   the Identity Generator device **characterized in that** the user's service indicator (USI) is opaque outside the Identity Generator device, which further comprises:

   – a Decomposer component (7) having means for carrying out a reverse generation (F^{-1}) to obtain a master user's identifier (UID) from a given user's service indicator (USI); and

   – means for verifying the validity of the given user's service indicator (USI) by making use of the master user's identifier (UID) as a search key towards the user directory system (4).

2. The Identity Generator device of claim 1, wherein the service identifier (SID), indicative of services to be accessed at the service provider, comprises at least one element selected from: a service provider indicator (SPI), and a number of service indicators (S1I; SMI).

3. The Identity Generator device of claim 1, further comprising:

- means for obtaining at least one element selected from: network operator identifier (OID), auxiliary value (Salt), expiry time, and integrity code; and
- means for including the at least one element into the user's service indicator (USI).

4. The Identity Generator device of claim 1, wherein the master user's identifier (UID) is built up as function (SHA-1) of a real user identity (MSISDN).

5. The Identity Generator device of claim 1, further comprising means for carrying out a symmetric cipher of the user's service indicator (USI) using a ciphering key (K_E).

6. The Identity Generator device of claim 5, wherein the ciphering key (K_E) is unique for all the applicable service providers (1; 2; 3).

7. The Identity Generator device of claim 5, wherein the ciphering key (K_E) is different per each service provider (1; 2; 3).

8. The Identity Generator device of claim 1, wherein the means for carrying out a reverse generation (F^{-1}) in the Decomposer component (7) includes means for obtaining the service identifier (SID) used to generate the given user's service indicator (USI).

9. The Identity Generator device of claim 1, wherein the means for carrying out a reverse generation (F^{-1}) in the Decomposer component (7) may further include means for obtaining at least one element selected from: network operator identifier (OID), and ciphering key (K_E) used to generate the given user's service indicator (USI).

10. The Identity Generator device of claim 1, wherein the means for carrying out a reverse generation (F^{-1}) in the Decomposer component may further include:

- means for obtaining applicable expiry time criteria; and
- means for verifying the validity of a given temporary user's service indicator (T-USI) against said expiry time criteria.

11. A method for generating at an Identity Generator device (6) of a network operator (IDP) a user's service indicator (USI) intended for a user (5) to access a number of services offered by a service provider (1; 2; 3) through a network operator where user data (4) for the user are accessible in a user directory system (4), this user's service indicator being usable between the service provider (SP-1; SP-2; SP-N) domain and the network operator (IDP) domain to unambiguously identify the user at each respective domain, the method comprising:

- a step of obtaining a master user's identifier (UID) usable to identify the user (5) at the operator's network;
- a step of obtaining a service identifier (SID), indicative of services to be accessed at the service provider; and

- a step of constructing a user's service indicator that includes the master user's identifier and the service identifier;

and the method **characterized in that** the constructed user's service indicator (USI) is opaque outside the Identity Generator device, and in that the method also comprises:

- a step of carrying out a reverse generation (F^{-1}) to obtain the master user's identifier (UID) from the given user's service indicator (USI); and

- a step of verifying the validity of the given user's service indicator (USI) by making use of the master user's identifier (UID) as a search key towards the user directory system (4).

12. The method of claim 11, wherein the step of obtaining a service identifier (SID) includes a step of obtaining at least one element selected from: a service provider indicator (SPI), and a number of service indicators (S1I; SMI).

13. The method of claim 11, further comprising:

- a step of obtaining at least one element selected from: network operator identifier (OID), auxiliary value (Salt), expiry time, and integrity code; and

- a step of including the at least one element into the user's service indicator (USI).

14. The method of claim 11, wherein the step of obtaining a master user's identifier includes a step of applying a function (SHA-1) to a real user identity (MSISDN).

15. The method of claim 11, further comprising a step of carrying out a symmetric cipher of the user's service indicator using a ciphering key (K_E).

16. The method of claim 15, wherein the ciphering key (K_E) is unique for all the applicable service providers.

17. The method of claim 15, wherein the ciphering key (K_E) is different per each service provider.

18. The method of claim 17, further comprising a step of determining a service provider issuing a communication based on a given user's service indicator.

19. A use of the Identity Generator device (6) of claim 1 integrated in, or in close co-operation with, an entity of an identity provider (IDP) network where the user data are accessible.

20. The use of claim 19, wherein the entity is a Central Provisioning Entity responsible for provisioning tasks in the operator's network.

21. The use of claim 19, wherein the entity is a User Directory System (4) storing user data.

22. The use of claim 19, wherein the entity is a Border Gateway placed at the border of the operator domain.

23. The use of claim 22, wherein the Border Gateway is an entity selected from: an HTTP Proxy, a WAP Gateway, and a Messaging Gateway.